ANR LYRICS: Cryptographie pour la protection de la vie privée, optimisée pour les services mobiles sans contact

Sébastien Gambs, Jean-François Lalande, Jacques Traoré

ANR LYRICS:
Cryptographie pour la protection de la vie privée, optimisée pour les services mobiles sans contact

Sébastien Gambs[*], Jean-Francois Lalande[+*], and Jacques Traoré[‡]

[*] *Université de Rennes 1, Inria, SUPELEC, CNRS, IRISA, UMR 6074, F-35065 Rennes, France*
[+] *INSA Centre Val de Loire, Univ. Orléans, LIFO EA 4022, F-18020 Bourges, France*
[‡] *Orange Labs, F-14066 Caen, France*

26 janvier 2015

Les smartphones de la prochaine génération intégreront la technologie NFC (communication sans contact en champ proche). Cette technologie permettra la dématérialisation de pièces justificatives liées à l'identité qui sont utilisées couramment dans la vie de tous les jours comme les tickets électroniques, les abonnements mensuels de transport, les cartes de crédit et de fidélité, les badges d'accès ou encore le permis de conduire. Un des risques inhérents à cette dématérialisation est celui de la gestion des données personnelles que ces services seront amenés à manipuler. Ainsi certains actes qui sont actuellement sans risques pour la vie privée s'ils sont payés en espèces, comme par exemple acheter une place de cinéma ou un ticket de bus, risquent de ne plus l'être une fois dématérialisés à cause des possibilités de traçage automatique.

L'ANR LYRICS [1], qui se termine en mai 2015, a pour objectif principal de fournir des services mobiles sans contact sécurisés et garantissant le respect de la vie privée de leurs utilisateurs, c'est-à-dire sans avoir à révéler leur identité ou toute autre information personnelle non requise par le service. Pour ce faire, l'ANR LYRICS a conçu de nouvelles solutions assurant deux des principes fondamentaux en matière de protection de la vie privée : la minimisation des données (qui stipule que seules les informations strictement nécessaires pour réaliser le service devront être divulguées et rien de plus) et la souveraineté des données (qui affirme que les données personnelles reliées à un individu lui appartiennent, et qu'il doit pouvoir contrôler la manière dont ses données sont utilisées).

De nouvelles primitives cryptographiques ont ainsi été créées qui permettent notamment de concilier deux propriétés qui peuvent sembler antagonistes *a priori* : l'authentification (seules les personnes autorisées doivent pouvoir accéder à un service particulier) et le respect de la vie privée (l'anonymat de l'utilisateur du service ainsi que la non-chaînabilité de ses actions doivent être garanties, même vis-à-vis du fournisseur du service lui-même). Ces nouveaux protocoles sont adaptés aux contraintes (mémoire et puissance de calcul limitées) des téléphones portables et des cartes SIM actuelles munies de la technologie NFC. En particulier, afin de gagner en efficacité, certaines des solutions développées délèguent des parties non-critiques des calculs cryptographiques effectués par la SIM (c'est-à-dire ne dévoilant pas d'éléments secrets) au téléphone mobile.

Trois cas d'usages ont été étudiés pendant la durée du projet, qui ont conduit au développement de trois démonstrateurs :

1. `https://projet.lyrics.orange-labs.fr`

— *Cas d'usage transport*. Le premier démonstrateur est un pass de transport anonyme et non-chaînable, similaire au pass Navigo, et qui permet de s'authentifier comme porteur d'un abonnement avec une borne NFC. La difficulté majeure de ce cas d'étude est le respect de la contrainte des 300 millisecondes maximum, imposée par les opérateurs de transport, pour la durée du protocole d'authentification entre le mobile NFC et la borne.
— *Cas d'usage monnaie électronique*. Le deuxième démonstrateur est un porte-monnaie électronique, similaire au porte-monnaie Monéo, mais intégré à un mobile NFC et offrant de bien meilleures garanties en termes de sécurité, de respect de la vie privée et d'expérience utilisateur.
— *Cas d'usage identité numérique*. Le troisième démonstrateur illustre la mise en œuvre d'un système d'accréditations anonymes au travers de divers services de la vie quotidienne (consultations locales, accès à la bibliothèque ou à la piscine, etc.). Le système proposé permet à un utilisateur d'obtenir des accréditations certifiées (permis de conduire, carte de vie quotidienne, permis d'étudiant, carte d'assurance maladie, etc.) auprès d'organisations émettrices (préfecture, mairie, université, sécurité sociale, etc.), puis de prouver ensuite la possession de ces accréditations auprès de fournisseurs de services tout en minimisant l'information dévoilée. Ainsi, un utilisateur pourrait par exemple prouver qu'il est étudiant et qu'il a moins de 25 ans, afin de bénéficier d'un tarif préférentiel à l'entrée d'un musée, sans révéler sa date de naissance ou son numéro de carte étudiant.

Les mécanismes cryptographiques à bas coût pour la protection de la vie privée ainsi que leur mise en œuvre dans les différents cas d'usage ont été présentés dans des conférences internationales, telles que EuroPKI 2013 [1], AsiaCCS 2013 [2], ICICS 2013 [3], MobiCase 2013 [4], CANS 2014 [5] et PKC 2015 [6], ou encore à des salons comme Cartes 2013 ou NFC World Congress 2013.

Dans le cadre de la conférence RESSI, nous proposons de faire une synthèse des résultats de LYRICS et de les illustrer au travers d'une ou deux démonstrations.

Références

[1] S. Canard, I. Coisel, A. Jambert, and J. Traoré, "New results for the practical use of range proofs," in *Public Key Infrastructures, Services and Applications* (S. Katsikas and I. Agudo, eds.), vol. 8341 of *Lecture Notes in Computer Science*, (Egham, UK), pp. 47–64, Springer Berlin Heidelberg, 2013.

[2] S. Gambs, C. Onete, and J.-M. Robert, "Prover anonymous and deniable distance-bounding authentication," in *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, ASIA CCS '14, pp. 501–506, Kyoto, Japan, 2014.

[3] S. Canard, I. Coisel, J. Devigne, C. Gallais, T. Peters, and O. Sanders, "Toward generic method for server-aided cryptography," in *Information and Communications Security* (S. Qing, J. Zhou, and D. Liu, eds.), vol. 8233 of *Lecture Notes in Computer Science*, (Beijing, China), pp. 373–392, Springer International Publishing, 2013.

[4] G. Arfaoui, S. Gambs, P. Lacharme, J.-F. Lalande, L. Roch, and J.-C. Paillès, "A Privacy-Preserving Contactless Transport Service for NFC Smartphones," in *Fifth International Conference on Mobile Computing, Applications and Services* (G. Memmi and U. Blanke, eds.), vol. 130 of *LNICST*, (Paris, France), pp. 282–285, Springer Berlin / Heidelberg, 2013.

[5] N. Desmoulins, R. Lescuyer, O. Sanders, and J. Traoré, "Direct anonymous attestations with dependent basename opening," in *Cryptology and Network Security* (D. Gritzalis, A. Kiayias, and I. Askoxylakis, eds.), vol. 8813 of *Lecture Notes in Computer Science*, (Heraklion, Greece), pp. 206–221, Springer International Publishing, 2014.

[6] S. Canard, D. Pointcheval, O. Sanders, and J. Traoré, "Divisible e-cash made practical," in *18th International Conference on Practice and Theory in Public-Key Cryptography (PKC '15)*, Lecture Notes in Computer Science, (Gaithersburg, USA), Springer-Verlag, 2015. To appear.